

Державний вищий навчальний заклад  
«Донецький національний технічний університет»  
Кафедра Прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

\_\_\_\_\_ Леонід Бачурін

«\_\_\_\_\_» \_\_\_\_\_ 2024 р.

## РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВБ1.4 Методи приховування інформації

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність (ості) 125 Кібербезпека

(шифр і назва спеціальності (тей))

Освітня програма 125 Кібербезпека

(назва освітньої програми, для обов'язкових дисциплін)

Мова навчання: українська

Робоча програма навчальної дисципліни «Методи приховування інформації»

для здобувачів вищої освіти за спеціальністю 125 Кібербезпека

2024 рік. – 8 с.

Розробник:

Александрова О.В., ас. каф. ПМІ

Александров М.О., доктор філ. зі спец. «Комп'ютерні науки», доц. кафедри ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики  
Протокол № 13 від. “27” грудня 2023 р.

Завідувач кафедри прикладної математики та інформатики

\_\_\_\_\_ (Маслова Н.О.)  
(підпис) (прізвище та ініціали)  
“ 27 ” \_\_\_\_\_ 12 \_\_\_\_\_ 2023 р.

Схвалено науково-методичною комісією з галузі знань \_\_\_\_\_ 12 Інформаційні технології \_\_\_\_\_  
(шифр, назва)  
Протокол № 1 від. “15” січня 2024 р.

“ 15 ” \_\_\_\_\_ 01 \_\_\_\_\_ 2024 р. Голова \_\_\_\_\_ (Башков Є.О.)  
(підпис) (прізвище та ініціали)

## 1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	Вибіркова дисципліна	
Обсяг в кредитах ЄКТС	5	
Обсяг в годинах за навчальним планом, разом: в тому числі:	150	
лекцій:	32	
практичні заняття:	-	
лабораторні заняття:	32	
семінари:	-	
самостійна робота:	86	
Форма підсумкового контролю	<u>Екзамен</u>	
Дисципліну викладають	Викладачі: Александров Микита Олександрович, Александрова Олександра Василівна, mykyta.aleksandrov@donntu.edu.ua oleksandra.aleksandrova@donntu.edu.ua	

**Передумови для вивчення дисципліни:** перелік дисциплін, які мають бути вивчені раніше: «Дискретна математика», «Вища математика», «Програмування», «Чисельні методи».

## 2. Мета вивчення навчальної дисципліни

Для обов'язкових дисциплін стисло зазначити місце навчальної дисципліни в освітній програмі та компетентності та результати навчання, для формування яких вона використовується.

### Компетентності:

- Здатність аналізувати предметні області (домени), формулювати вимоги, ідентифікувати, класифікувати та описувати завдання, знаходити методи й підходи до їх розв'язання.
- Знання і розуміння специфікацій, стандартів, правил і рекомендацій в професійній галузі, уміння оцінювати ступінь обґрунтованості їх застосування, здатність дотримуватися їх при реалізації процесів життєвого циклу.
- Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.
- Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.

### Програмні результати навчання:

- Розробляти моделі загроз та порушника.
- Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
- Забезпечувати неперервність процесу ведення журналів реєстрації подій, та інцидентів на основі автоматизованих процедур.

- Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

- Вміння використовувати інформаційні та комунікативні технології при спілкуванні, обміні, зборі, аналізі, обробці інформації.

- Розуміти, аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

- Знати, розуміти і застосовувати сучасні підходи щодо оцінки та забезпечення якості програмного забезпечення.

- Знати, розуміти, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем

### **3. Очікувані результати навчання**

(для обов'язкових дисциплін)

Формулювання результатів навчання має базуватись на програмних результатах навчання, визначених відповідною освітньою програмою та деталізувати їх.

Формулювання результатів навчання мають визначати рівень їх сформованості, наприклад, через їх достатність для вирішення певного класу завдань професійної діяльності та/або подальшого навчання за освітньою програмою.

### **4. Засоби діагностики результатів навчання**

Засобами оцінювання та методами демонстрування результатів навчання можуть бути:

- екзамени;
- стандартизовані тести;
- індивідуальні та командні проекти;
- аналітичні звіти, реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- виступи на наукових заходах;
- завдання на лабораторному обладнанні або на реальних об'єктах;
- інші види індивідуальних та групових завдань.

### **5. Критерії оцінювання результатів навчання**

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

ЛР 1	ЛР 2	ЛР 3	ЛР 4	ЛР 5	ЛР 6	Поточний контроль	Екзамен	Максимальний бал
5	5	5	5	10	10	40	60	100
3	3	3	3	6	6	24		

Примітки: 1) ЛР 1, ЛР 2 і т.д. лабораторні роботи;

2) У чисельнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоечасному виконанні)

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту(роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

## 6. Програма навчальної дисципліни

### 6.1. Основні теми дисципліни

**Тема 1.** Поняття інформаційної безпеки. Сучасні підходи до шифрування інформації. Модульна арифметика. Модель загрози та порушника. Інциденти.

**Тема 2.** Шифри, які засновані на модульній арифметиці. Поняття симетричних шифрів.

**Тема 3.** Симетричні (одноключові) шифри. Моноалфавітні шифри. Шифр Цезаря – адитивний, мультиплікативний, афінний.

**Тема 4.** Симетричні (одноключові) шифри. Багатоалфавітні шифри. Автоключовий шифр. Шифр Віженера. Шифр Плейфера. Шифр Хіла.

**Тема 5.** Одноключеві шифри. Шифри підстановок, перестановок, гамування, квантові. Шифр Вернама. Квадрат Полібія.

**Тема 6.** Блокові шифри. Шифри на основі мережі Фейстеля. Data Encryption Standard (DES).

**Тема 7.** Блокові шифри. Advanced Encryption Standard (AES). Режими блочного шифрування.

**Тема 8.** Забезпечення безпеки елементів інформаційно-телекомунікаційних систем. Поточкові шифри. Генератори псевдовипадкових чисел. Шифри RC4, SNOW, STRUMOK.

**Тема 9.** Поняття цифрової стеганографії. Модель стеганосистеми та її види. Поняття ЦВЗ.

**Тема 10.** Стеганографічні методи приховування інформації. Метод заміни найменш значущого біта. Поєднання стеганографічних та криптографічних методів.

### 6.2. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Проведення практичних занять не передбачено		
...	Усього годин		

### 6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Модульна арифметика. Алгоритм Евкліда. Розширений алгоритм Евкліда	4	
2	Шифр підстановок. Використання адитивного алгоритму.	4	
3	Використання багатоалфавітних шифрів. Автоключовий шифр. Шифр Віженера. Шифр Плейфера.	4	
4	Запрограмування шифру Гіла. Мануальне використання шифру Вернама та квадрату Полібія.	4	

5	Мануальний розрахунок раунду DES. Запрограмування та аналіз DES.	8	
6	Приховування даних у просторовій області зображення. Метод заміни найменш значущого біта в поєднанні з криптографічними методами.	8	
...	<b>Усього годин</b>	32	

#### 6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Тема 1. Поняття інформаційної безпеки. Сучасні підходи до шифрування інформації. Модульна арифметика. Модель загрози та порушника. Інциденти.	9	
2	Тема 2. Шифри, які засновані на модульній арифметиці. Поняття симетричних шифрів.	8	
3	Тема 3. Симетричні (одноключові) шифри. Моноалфавітні шифри. Шифр Цезаря – адитивний, мультиплікативний, афінний.	9	
4	Тема 4. Симетричні (одноключові) шифри. Багатоалфавітні шифри. Автоключовий шифр. Шифр Віженера. Шифр Плейфера. Шифр Хіла.	8	
5	Тема 5. Одноключеві шифри. Шифри підстановок, перестановок, гамування, квантові. Шифр Вернама. Квадрат Полібія.	8	
6	Тема 6. Блокові шифри. Шифри на основі мережі Фейстеля. Data Encryption Standard (DES).	8	
7	Тема 7. Блокові шифри. Advanced Encryption Standard (AES). Режими блочного шифрування.	9	
8	Тема 8. Забезпечення безпеки елементів інформаційно-телекомунікаційних систем. Поточкові шифри. Генератори псевдовипадкових чисел. Шифри RC4, SNOW, STRUMOK.	9	
9	Тема 9. Поняття цифрової стеганографії. Модель стеганосистеми та її види. Поняття ЦВЗ.	9	
10	Тема 10. Стеганографічні методи приховування інформації. Метод заміни найменш значущого біта. Поєднання стеганографічних та криптографічних методів.	9	
...	<b>Усього годин</b>	86	

#### 6.5. Індивідуальні та/або групові завдання

У рамках курсу для студентів денної форми навчання виконання індивідуальної роботи не передбачено.

## **7. Література**

### **7.1. Основна**

1. Онацький О. В., Йона Л. Г. Криптографічні системи : навчальний посібник з дисциплін "Криптографія та криптоаналіз" для освітньо-професійної підготовки бакалаврів в галузі знань 12 "Інформаційні технології" за спеціальністю 125 "Кібербезпека" / О. В. Онацький, Л. Г. Йона. – Одеса : Міжнародний гуманітарний університет, 2023. – 156 с.
2. Мисло Ю. М. Елементи математичних методів у криптології: навч. посіб. для студентів спеціальності «Кібербезпека та захист інформації»/ Ю. Мисло, М. Пагіря, В. Різак. — Ужгород: Говерла, 2023. — 136 с.
3. Теорія та практика розслідування злочинів в умовах протидії: навч.-метод. Посібник / Аркуша, Л. І., Гуртієва, Л. М., Д'ячкова, М. О., Загородній, І. В., Мурзановська, А. В., Підгородинська, А. В., & Торбас, О. О. – Одеса: Фенікс, 2021.
4. Вишняков, В. М. Захист інформації в комп'ютерних системах : навч. посібник / В. М. Вишняков ; Київ. нац. ун-т буд-ва і архіт. - Київ : КНУБА, 2022. - 119 с.
5. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с
6. Стасєв Ю. В., Козюберда К. В., Кулабухов О. М. Аналіз методу приховування інформації від несанкціонованого доступу на основі стеганографічного перетворення. Збірник наукових праць Харківського національного університету Повітряних Сил. 2023. № 3 (77). С. 57-61
7. Нога О. В. Методи стеганографічного захисту і стеганоаналізу інформації з використанням аудіофайлів: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / О. В. Нога. – Тернопіль : ТНТУ, 2022. – 52 с.
8. Безпека інформаційних систем [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», освітня програма «Цифрові технології в енергетиці» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,98 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2023. – 161 с.
9. Методологія і технології захисту інформації: навчальний посібник / А.Н. Аль-Амморі, Н.М. Наумова, П.В. Дяченко, Р.М. Іщенко, М.М. Дехтяр, А.Є. Ключан; НТУ. – Київ: НТУ, 2020. – 147с.

### **7.2. Допоміжна**

1. Туровський, О., Лазаренко, С., Щербак, Т., Рябова, Л., & Мелешко, Т. (2022). Методика оцінки стеганографічних методів приховування інформації в зображеннях. Інфокомунікаційні та комп'ютерні технології, 2(02). <https://doi.org/10.36994/2788-5518-2021-02-02-23>
2. Фаль О. М. Криптографія: основні ідеї та застосування/ О. М. Фаль. – К.: Вид-во НТТУ КПІ, 2004.
3. Антонюк А.О. Основи захисту інформації в автоматизованих системах/ А. О. Антонюк. – К.: КМ Академія, 2006. – 244 с. Вербіцький О.В. Вступ до криптології/ О. В. Вербіцький. – Львів: Вид-во НТЛ, 2008. - 248 с.
4. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. - К.: Держстандарт України, 1998.

5. Закон України «Про державну таємницю». – К.: Відомості Верховної Ради України, 1994. - N 16. - Ст. 93.
6. Закон України «Про захист інформації в інформаційно телекомунікаційних системах». – К.: Відомості Верховної Ради України, 1994. - N 31. - Ст. 286.
7. Закон України «Про інформацію». – К.: Відомості Верховної Ради України, 1992. - N 48. - Ст. 650
8. Закон України «Про електронний цифровий підпис». – К.: Відомості Верховної Ради України, 2003. - N 36. - Ст. 276.
9. Інформаційна безпека комп'ютерних систем і мереж: Методичні вказівки // Укл. А.Ф. Карачка, М.П. Карпінський, А.В. Кулик, Т.В. Лендюк. – Тернопіль: ТАНГ, 2007. – 68 с
10. Пономаренко В. С. Основи захисту інформації. Навчальний посібник / В. С. Пономаренко, І. В. Журавльова. – Харків: Вид. ХДЕУ, 2003. – 176 с.
11. Кузнецов О. О. Стеганографія : навчальний посібник / О.О.Кузнецов, С. П. Євсєєв, О. Г. Король. // – Х. : Вид. ХНЕУ, 2011. – 232с.
12. Конахович Г. Ф. Комп'ютерна стеганографія. Теорія і практика / Г. Ф. Конахович, А. Ю. Пузиренко. – К. : "МК-Пресс", 2006. – 288 с.
13. Основи комп'ютерної стеганографії : навч. посібн. для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. В. Шелест та ін. – Вінниця : ВДТУ, 2003. – 143 с.
14. Бабенко В.Г., Зажома В.М., Нестеренко О.Б.. Метод вбудовування стегоповідомлення на основі ключового елемента / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко. // Захист інформації. 2014. С. 53-58
15. Attack Modelling: Towards a Second Generation Watermarking Benchmark / S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun. // Preprint. University of Geneva, 2001. – 58 p.
16. Westfeld A. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools – and Some Lessons Learned / A. Westfeld, A. Pfitzmann // Proceeding of the Workshop on Information Hiding. – 1999.

### **7.3. Методична**

1. Методичні вказівки до виконання практичних завдань з дисципліни «Методи приховування інформації» 125 Кібербезпека (у розробці).

## **8. Інформаційні ресурси**

1. Види шифрування інформації [Електронний ресурс]. – Режим доступу : <https://ua5.org/protect/395-vidi-shifruvannya-informaciyi.html>
2. Що таке стеганографія і чим вона відрізняється від криптографії [Електронний ресурс]. – Режим доступу : <https://instagalleryapp.com/informacijna-bezpeka/shho-take-steganografija-ta-chim-vona/>
3. Історія розвитку стеганографії [Електронний ресурс]. – Режим доступу : <https://studfile.net/preview/9650053/>
4. Стеганографічний алгоритм захисту даних з використанням файлів зображень [Електронний ресурс]. – Режим доступу : <http://www.economy.nayka.com.ua/?op=1&z=5584>